DETAILED ACTION

Amendment

1. Receipt is acknowledged of the Amendment filed July 10, 2008.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gercekci et al (4,841,133), hereinafter Gercekci in view of Vogt et al (2004/0078511), hereinafter Vogt.

With respect to claim 1, Gercekci discloses in the abstract an unauthorized access prevention method for an integrated circuit (also referred to as a "smart card", i.e., integrated circuit – regarding claim 10) including a plurality of resistor elements (fuse 28) capable of selecting between a high and low impedance state irreversibly in an interface portion within the integrated circuit. Furthermore Gercekci discloses that when an invalid keyword (externally-applied code) is input at least once, the access is judged as being an unauthorized access and the impedance state of the resistor element (fuse) is changed from an initial state to stop a part or all of accesses to the integrated circuit irreversibly.

Specifically as is taught in the abstract, the resister element is "blown" when two codes, i.e., signals (preprogrammed transport code and an externally-applied code) do

not match. It is understood that when a fuse is blown it has a relatively high impedance compared to the fuse having an unblown state.

It is further disclosed in column 1, lines 37-39 that an object the present invention to provide an increased level of security against the theft of un-initialized cards.

Gercekci's teachings above fail to specifically disclose that the invalid keyword (externally-applied code) must be inputted exactly three times in a row in order to be judged as being an unauthorized access.

With respect to claim 1, Vogt discloses in paragraph 0076, that in order to limit the chance of a successful attack of hidden memory storage, one must limit the number of password guesses allowed without penalty. It is further disclosed that "The suggested approach is to allow three consecutive incorrect password entries before disabling access to hidden storage. For example user 1 enters his password incorrectly two consecutive times. If the password is entered correctly on the third attempt, user 1 is granted access to user 1's hidden storage. If the password is entered incorrectly a third consecutive time, the access to user 1's space is permanently denied."

In view of Vogt's teachings, it would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to apply Vogt's method of limiting the number of password attempts, specifically to three attempts, to the unauthorized access prevention method taught by Gercekci. Gercekci teaches disabling the card when an invalid code is input at least once. One would be motivated to allow the user attempting to access the card/memory three opportunities in order to account for a user's unintentional mistake. By allowing three attempts, the user is granted some leeway yet

at the same time, the system prevents unauthorized users from having unlimited attempts to access the card/memory thereby maintaining security to the card/memory.

4. Claim 2, 9, 11, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gercekci in combination with Vogt and in further view of Dalton et al (2003/0080393), hereinafter Dalton.

Gercekci's teachings in combination with the teachings of Vogt are discussed above including the limitation of claims 11 and 18, that the unauthorized access prevention method is applied to an IC card. The combination however fails to specifically teach the resistor element containing an organic conductor.

With respect to claim 2, Dalton discloses in paragraph 0001, that the present invention relates generally to integrated circuit devices and, more particularly, to an encapsulated, energy-dissipative fuse for use with integrated circuit devices. Paragraph 0011 further a fuse structure (resistor element) wherein an organic material is encapsulated beneath a thin, conductive layer, thereby forming a fuse structure. Paragraph 0021 details an alternative structure wherein the organic material (such as Ormecon) is itself the conductive layer.

With regards to claim 9, Dalton teaches in paragraph 0002 discloses that the invention relates to semiconductor integrated circuits. It is further disclosed in Dalton's claim 18 that the semiconductor integrated circuit comprises electrically conductive organic material.

Lastly, Dalton explains in paragraph 0005 that using the described fuse, allows the blowing of the fuse with lower applied energy while still sufficiently ablating so as not to result in short circuiting of other components.

In view of Dalton's teachings, it would have been obvious to an artisan of ordinary skill in the art at the time the invention was made use the fuse taught by Dalton as the fuse used to prevent unauthorized access to an integrated circuit taught by Gercekci in combination with Vogt. Gercekci simply teaches using a fuse to deactivate the integrated circuit, however the specific fuse that is used is not disclosed. Dalton discloses that the fuse structure, which includes an organic conductor, is often used in integrated circuit devices and furthermore discloses that such a structure allows the blowing of the fuse with lower applied energy while still sufficiently ablating so as not to result in short circuiting of other components. Therefore in view of Dalton's teachings one would be motivated to use such a fuse so that the desired fuse is blown while maintaining the structure of the remaining circuit.

5. Claims 3 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gercekci in combination with Vogt and in further view of Cheng et al (2003/0060009), hereinafter Cheng.

Gercekci's teachings in combination with the teachings of Vogt are discussed above including the limitation of claim 12, that the unauthorized access prevention method is applied to an IC card. The combination however fails to specifically teach the resistor element being formed of a capacitor.

With respect to claim 3, Cheng illustrates in figures 1A-1H a metal capacitor and fuse structure formed. Paragraph 0002 discloses the advantage of fuses being formed with metal-insulator-metal capacitors, wherein the advantage is that such capacitors used in integrated structures possess the ability to precisely control their capacitance based on dimensional control.

In view of Chen's teachings, it would have been obvious to an artisan of ordinary skill in the art at the time the invention was made use the fuse, which is formed with a capacitor taught by Chen as the fuse used to prevent unauthorized access to an integrated circuit taught by Gercekci in combination with Vogt. Gercekci simply teaches using a fuse to deactivate the integrated circuit, however the specific fuse that is used is not disclosed. Chen discloses that the fuse structure, which includes a metal capacitor is often used in integrated circuit in order to precisely control the capacitance in the integrated circuit. Therefore in view of Chen's teachings one would be motivated to use such a fuse so that the capacitance of the integrated circuit can be precisely controlled. Furthermore forming the capacitor with the fuse allows for less parts.

6. Claims 4 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gercekci in combination with Vogt and in further view of Kurth et al (7,218,547).

Gercekci's teachings in combination with the teachings of Vogt are discussed above including the limitation of claim 13, that the unauthorized access prevention method is applied to an IC card. Although Gercekci in combination with Vogt teach securing the card by changing the impedance of the resistor element, the specific method of applying a higher voltage to the resistor element is not disclosed.

With respect to claim 4, Kurth discloses in column 2, lines 55-64, that the resistor element presents a high impedance between the conductive plates before being "blown" or programmed, and a relatively low impedance between the conductive plates after being programmed. To program the resistor element, a programming voltage of a sufficient magnitude is applied across the conductive plates causing a "breakdown" of the dielectric layer, which results in the dielectric layer having relatively low impedance. Kurth further discloses that resistor elements can be used in a variety of applications, including selectively enabling or disabling components on a semiconductor integrated circuit.

In view of Kurth's teachings, it would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to apply a higher voltage to the resistor element in order to change its impedance as is taught by Kurth, to the unauthorized access prevention method taught by Gercekci in combination with Vogt. Gercekci teaches preventing the use of a smart card by comparing an entered signal to a present signal and securing the card if the signals do not match. As is recited above, although Gercekci teaches securing the card by changing the impedance of the resistor element, the specific method of achieving the change of impedance is not disclosed. Kurth however specifically teaches achieving a change of impedance for the purpose of disabling components in an integrated circuit. Therefore one would be motivated to apply a higher than normal voltage to the resistor element since as is discussed by Kurth, doing such will result in changing the impedance of the element

and in turn will disable certain integrated circuit components and result in securing the integrated circuit.

7. Claims 5 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gercekci in combination with Vogt and in further view of Khoury (2003/0011379).

Gercekci's teachings in combination with Vogt are discussed above including the limitation of claim 14, that the unauthorized access prevention method is applied to an IC card. Although Gercekci in combination with Vogt teach securing the card by changing the impedance of the resistor element, the specific method of applying a larger current to the resistor element is not disclosed.

With respect to claim 5, Khoury discloses in paragraph 0002 using fuse or anti-fuse fusible links (resistor elements) wherein fuse links are opened by blowing the fuse by applying a writing current. It is further disclosed that once a fuse link is blown the impedance of the link is much higher than that of an unblown fuse. Paragraph 0025 refers to the action of applying current to blow a fuse as "Fuse-Current-Switch".
In view of Khoury's teachings, it would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to apply a large current to the resistor element (fuse) in order to change its impedance as is taught by Khoury, to the unauthorized access prevention method taught by Gercekci in combination with Vogt. Gercekci teaches preventing the use of a smart card by comparing an entered signal to a present signal and securing the card if the signals do not match. As is recited above, although Gercekci teaches securing the card by changing the impedance of the resistor element, the specific method of achieving the change of impedance is not

disclosed. Khoury however specifically teaches achieving a change of impedance (blowing a fuse) by applying current to the fuse. Therefore one would be motivated to apply a larger than normal current to the resistor element since as is discussed by Khoury, doing such will result in blowing the fuse and moreover disabling the circuit. Furthermore one would be motivated to use a Fuse-Current-Switch as they are commonly used and therefore is widely available and low in cost.

Response to Arguments

8. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new grounds of rejection. The previous Office action objected to claims 4 and 5 for informalities. Claims 4 and 5 have been amended to overcome the previous objections. Claims 7 and 8 were rejected under 35 U.S.C. 112, second paragraph. Claims 7 and 8 have been cancelled with the current amendment, thereby making the 112 rejection moot. Claim 1 has been amended to include the limitation, "when an invalid keyword is inputted three times in a row, the access is judged as being an unauthorized access." Applicants remark that prior art used in the previous Office action do not disclose the newly added feature. The Vogt reference is being provided however, which clearly teaches the added feature. Vogt's specific teachings are disclosed above as well are the reasons to combine Gercekci and Vogt in order to come up with the claimed invention. No further arguments are presented by the Applicant with regards to the specific rejections of claims 2-5, 9-14, and 18.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to *Allyson N. Trail* whose telephone number is (571) 272-2406. The examiner can normally be reached between the hours of 7:30AM to 4:00PM Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee, can be reached on (571) 272-2398. The fax phone number for this Group is (571) 273-8300.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [**allyson.trail@uspto.gov**].

All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

/Allyson N Trail/

Allyson N. Trail
Patent Examiner
Art Unit 2876

October 23, 2008